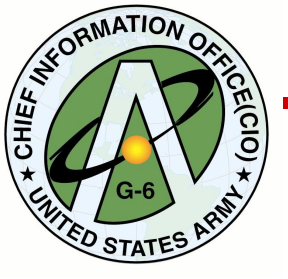


NETCOM / 9th Army Signal Command

Army Active Directory Status and Implementation Guidelines

Robert Bachert

Robert.bachert@us.army.mil

520-533-1855

Agenda

- Purpose
- Overview
- AD Guidelines
- AD In CONUS
- Implementation/Migration Planning
- Road Ahead

Purpose

- Provide an Active Directory status and emerging guidelines for planning and implementation.

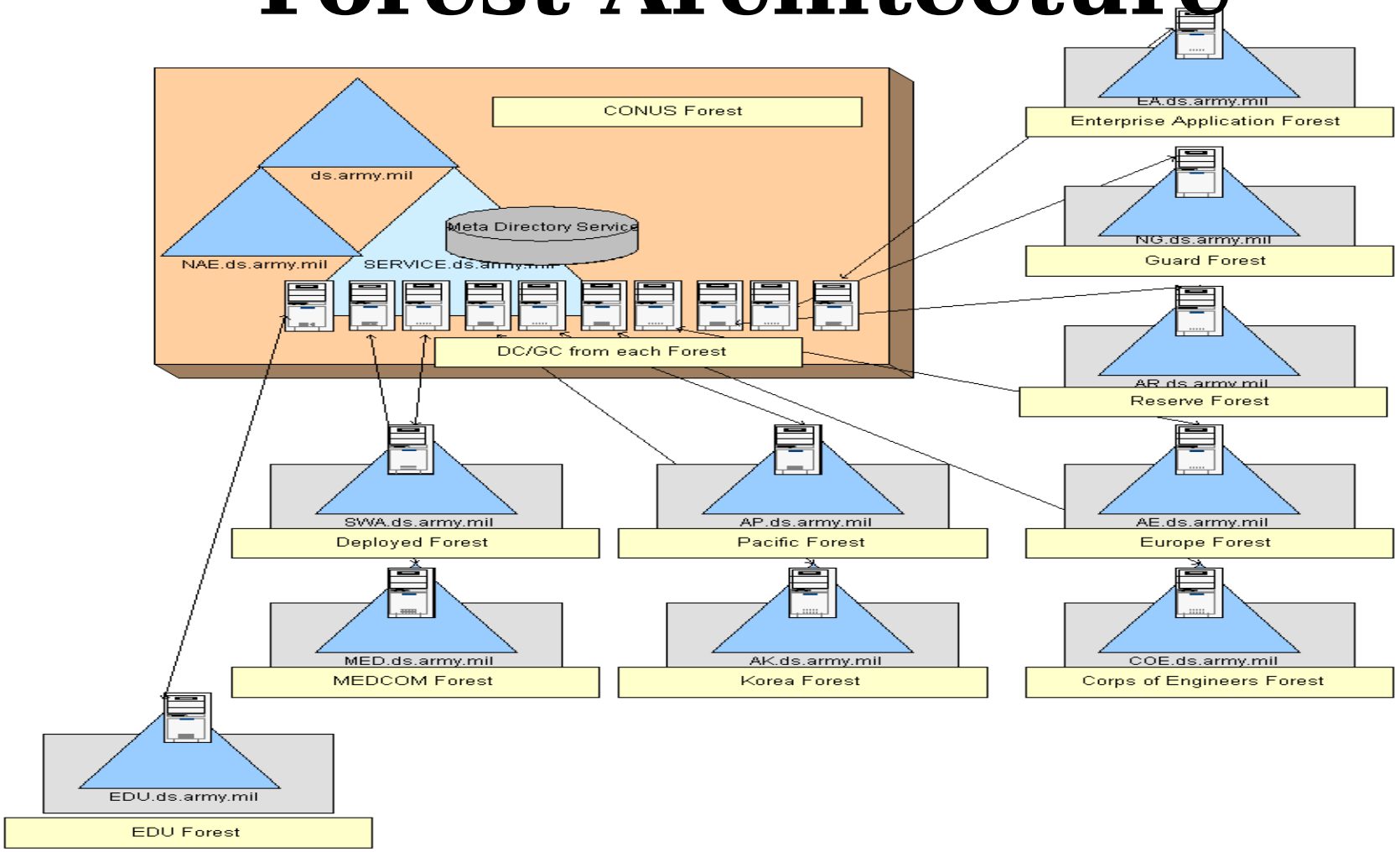
Technology is Driving Business

"The newest innovations, which we label information technologies, have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even five years ago."

Alan Greenspan

Chairman, US Federal Reserve

Army Active Directory Forest Architecture



Guidelines: Why AD?

- Microsoft support for NT 4.0 server ends Dec 04
- Army is currently ~95% NT 4.0
- Once Microsoft support ends, the Army is at risk
  - IAVA patches (requires separate support contract with Microsoft)
  - Reduced use of COTS software as commercial vendors stop producing software for the NT 4.0 environment
- Current NT 4.0 LAN-based architecture will not support the Objective Force/Net-centric Force
  - Highly segmented, isolated islands focused on local needs and security
  - Limited levels of trust and interoperability between domains
  - Labor intensive operations to support cross-LAN access
  - No ability to create a global Army directory of users and resources available for shared mission support
- All future Microsoft Operating Systems are AD enabled

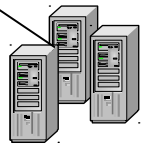
NT 4.0 Technology Replacement

NT member servers & User client OS's can Be replaced with Windows 2000 or better however some applications may not operate with Win2K OS

Must be upgraded to AD to provide Network OS

NT Network Domain Controllers

Network based upon Domain Controller OS



NT Member Server

Print, file, applicatio… etc

… Clients can be upgraded to Win 2K but if NT domain controllers Server OS's are replaced With Windows 2000 or better, The network is an Active Directory network

Exchange 5.5 operate as member server with Win2K OS within either NT 4.0 or AD Network environment.

(Researching)

User Clie…

Exchange 5.5 E-Mail

Conclusion:

A decision to get off of NT

Is a decision to implement

Active Directory.

AD Guidelines Sources

- AD Summits
  - Implementation Of AD in the Army
- AD Implementation Technical Guidance Package
  - Consists of eleven documents that
    - Provide customers guidance to get ready for AD and to implement an AD forest/domain or a top-level OU
    - Provide an organization with the required technical guidance needed to implement AD within the Army Enterprise Infostructure (AEI) environment.
- Master Configuration Cookbook
- Lessons learned (MDW, MEDCOM)

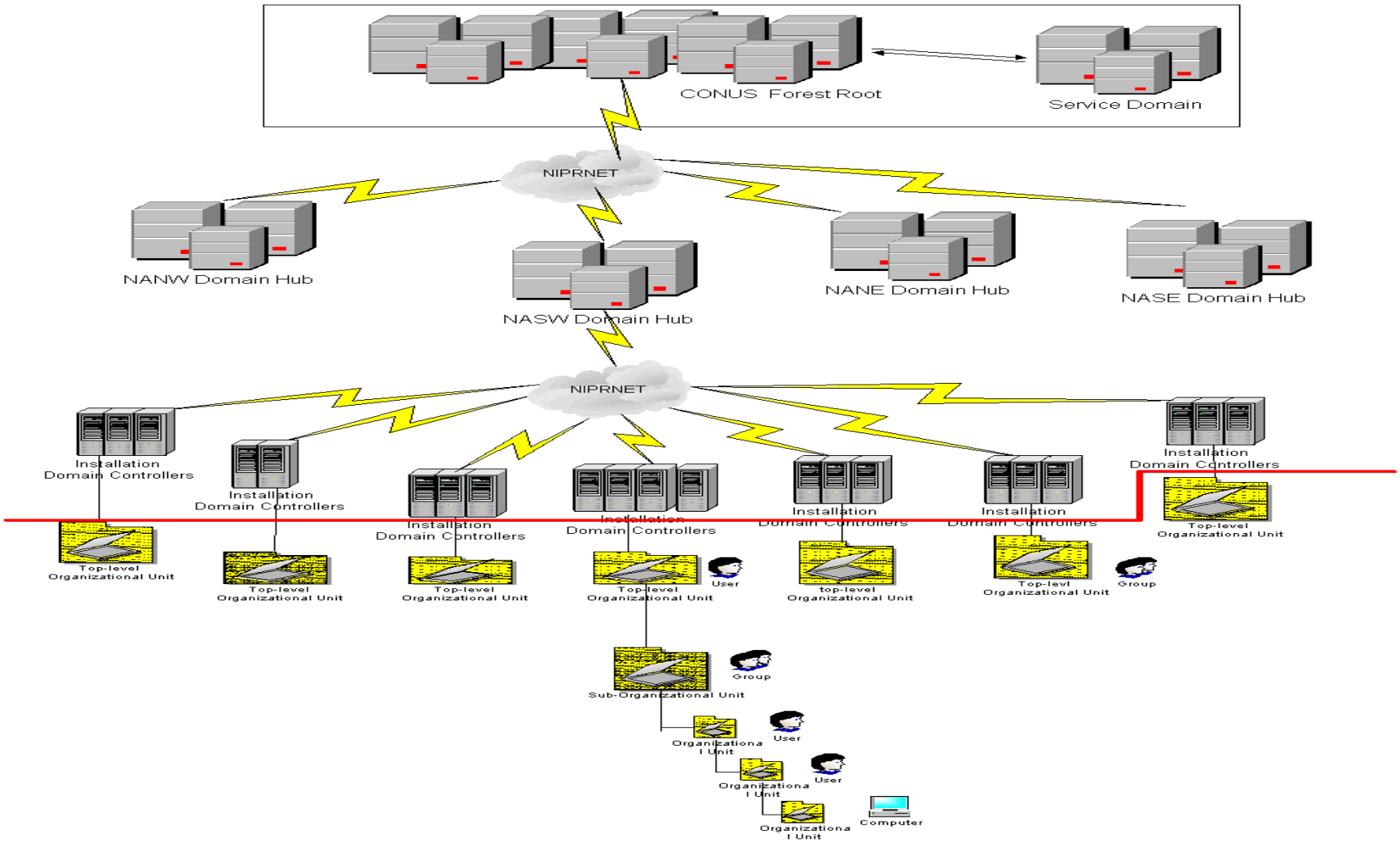
Guidelines: Role of AD

- Support LAN Client/Server operations (e.g., user authentication, printing, and sharing of files)
- Support Administration Delegation
- Support installation-level Exchange e-mail
  - Upgrade Exchange OS to Windows 2000
  - Decouple Exchange migration, target Exchange 2003
- Support Server Consolidation
- Standard Domain Controller Configuration
- Support Windows Server 2003 as the target Operating System (OS)
- Decouple from Army wide implementation of standard desktop OS

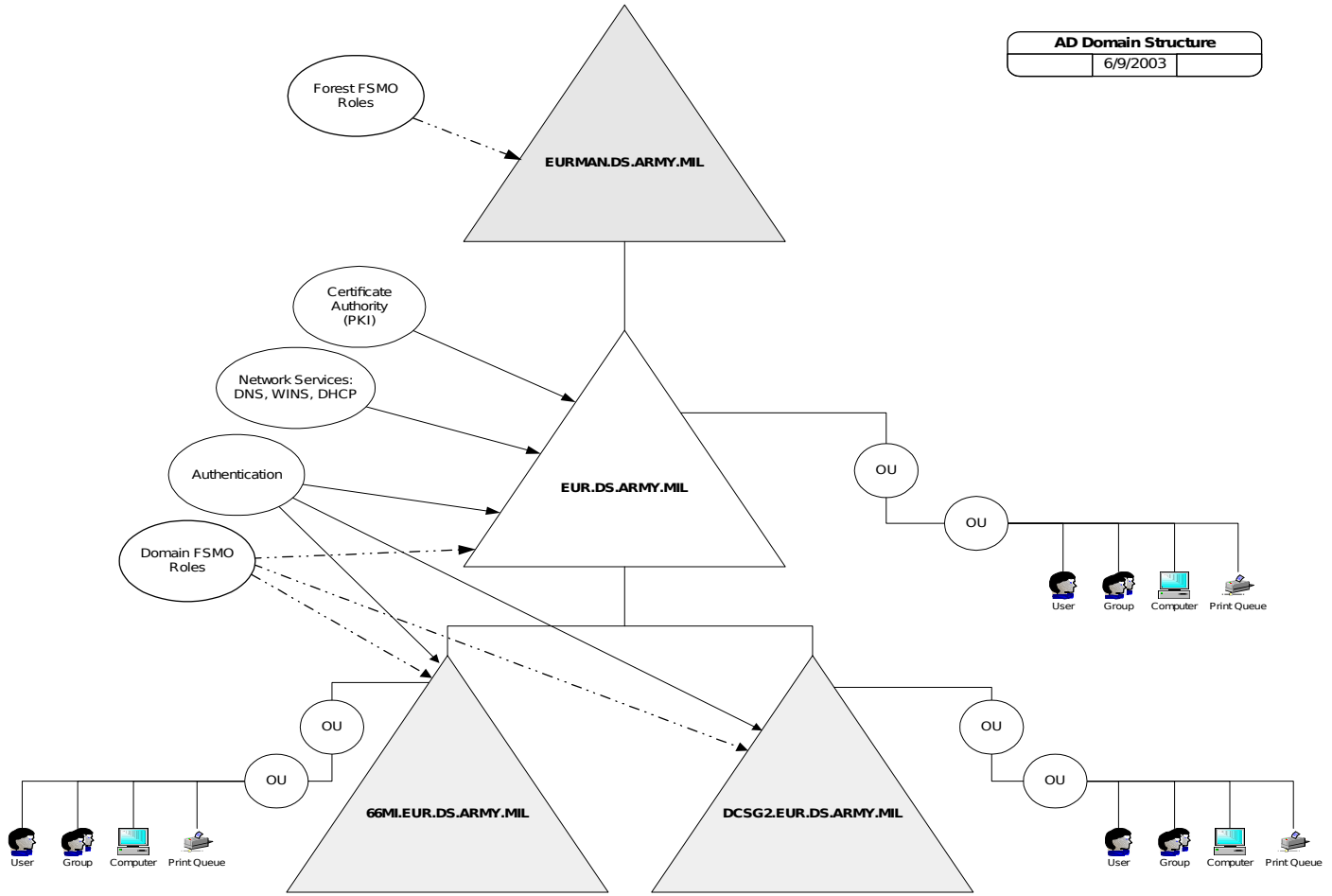
Role Of AD (Continued)

- Provide central control of AD Naming Convention and Schema and strict physical security / administration of AD Domain Controllers
- Secure AD sensitive traffic using IPSec - Under Review (ISEC)
- Microsoft Certificate Authority Design - Under Review (ISEC)
- Additional engineering required to design integrated security solution and resulting guideline for Army forests, domains, and sites

CONUS AD Structure



Europe AD Structure



AD Implementation

- Regional domains aligned to the IMA regions
- TNOSC manages regional domains using enterprise tools licensed for site support (domain controllers/critical servers)
- Site/installation support is migrated into an appropriate Organizational Unit (OU)
- OU structure operated under the Single DOIM Concept based on admin capabilities delegated from the TNOSC implementation/migration plan may further delegate selected responsibilities to lower level
- Domain Controllers in Secure Facilities (Physical Security)

Implementation Strategy

- NETCOM, PM DCACS/PM BES and AEI-Tech CCB Partnership
- Centralized management with decentralized execution
  - Possibility for AD Backbone centralized funding.
  - No centralized funding for site implementation
  - NETCOM approves Site Specific Implementation Plan (SSIP)
  - Centralized procurement of AD servers and software using core and installation funds
- Site Develops SSIP
  - Network Diagram
  - Migration plan
  - OU Structure
  - Resource Plan
- Four Phase Implementation Approach

NETCOM / 9th Army Signal Command

Four Phase Implementation

Pre-migration

Pre-Planni

- **Surveys**
- **SSIP**
- **Templates**

Phase 1
- **Establish "AD**

Phase 2
- **Extend AD to Sites**

Phase 3 & 4:
- **Implement SSIP**
- **Post Migration Actions**

PM/PC O & TNOSC

- **Establish Regional Hubs**
- **Review and approve SSIP**

PM/PC O & TNOSC

- **Installation DCs**
- **Populate Top-level OU**

PM/PC O & DOIM

- **Implement SSIP**
- **Migrate Computer accounts & users**

PM/PC O & DOIM

- **Post Migration**
- **Clean-up**
- **QA**

- **Configure DCs**
- **Acquire H/W & S/W**
- **Approve SSIP**
- **Seek Funds**

NETCOM with PM Support provides overall guidance and technical support during all phases

- **Templates**
- **Project Mgt Support**
- **Tech Support**

FY03

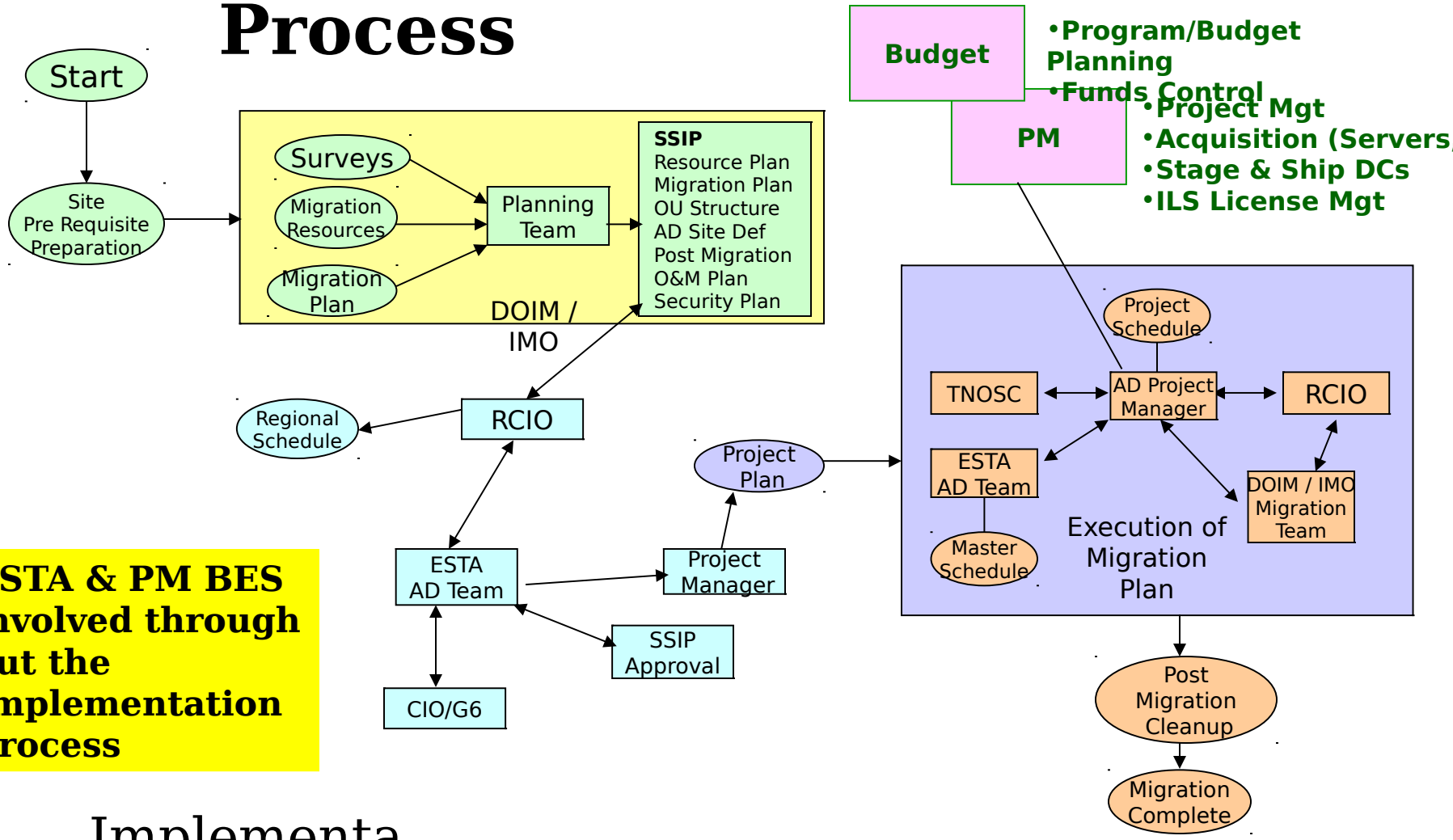
FY04

FY05

Migration Planning Considerations

- Assign a site lead
- Create public relations plan to educate Commanders, Directors, IMOs and users (Need Buy in from all)
- Develop communities of interest
- Develop an inventory
  - Status of NT Domain Consolidation
  - POCs/Administrators for Each Domain
  - Organizations/Users/Locations/IMO Contacts
  - Desktops (OS's, standard applications)
  - Network Topology and Devices (LAN/BAN/switches, hubs, cabling)
- Identify resources

Planning & Implementation Process



ESTA & PM BES involved through out the Implementation Process

Implementation Process

Resource Strategy

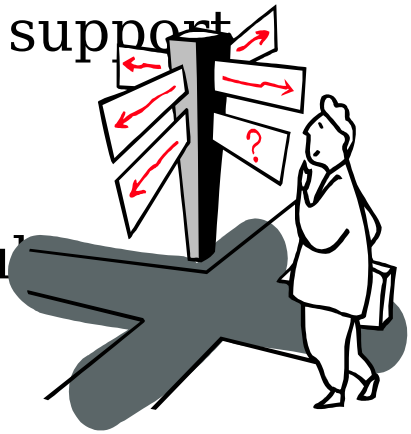
- Use the Resource plan to identify costs and shortfalls
- Consider projected reductions in total cost of ownership as an incentive for corporate investment
- Seek redistribution of funds from supported organizations
- Identify available Resources to aid in migration

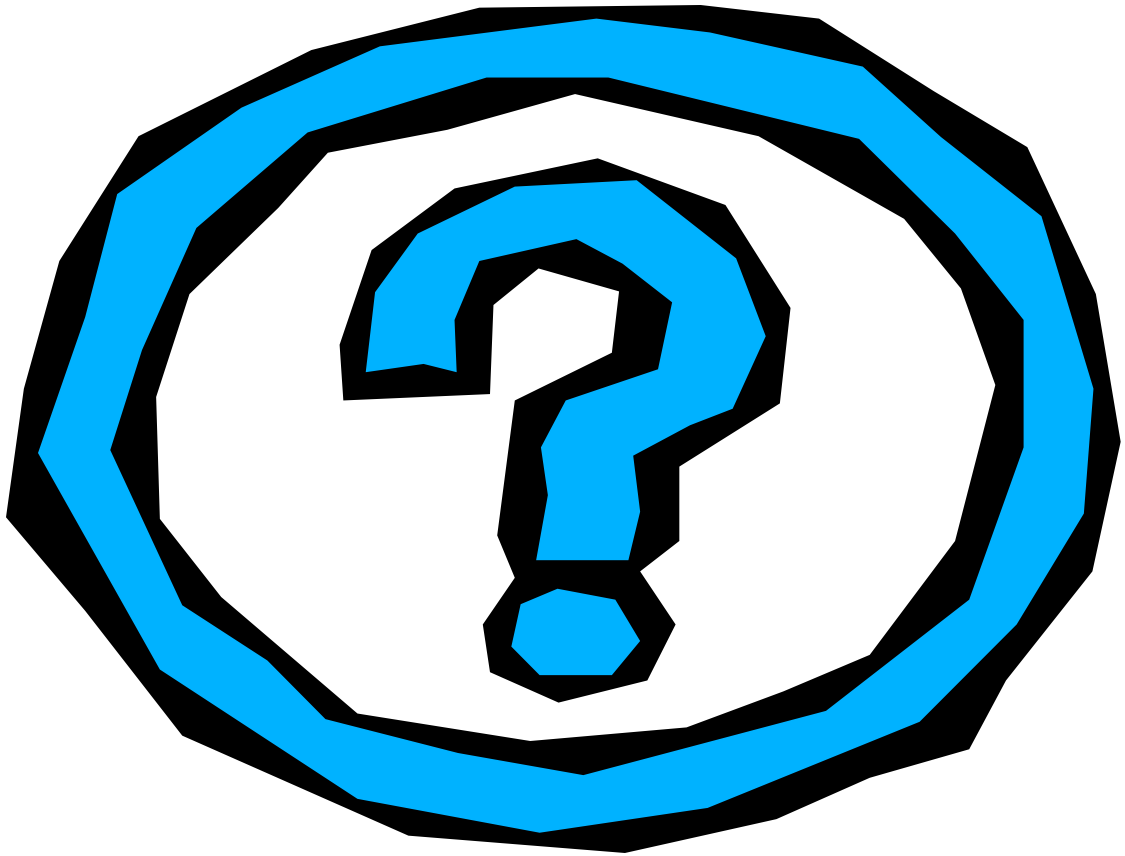
AD Implementation Cost

- NETCOM will work with IMAs and RCIOs to identify and program for the cost of the AD infostructure (DCs and enterprise operations).
- NETCOM is working with the CIO/G6 & PM BES to core fund the cost of O&M of all domain controllers.
- Need to develop an approach that addresses funding reallocation to resource the O&M of AD Site operations.

Road Ahead

- Develop a Regional Schedule for AD migration
- Prepare Servers and Desktops for AD Aware
- Work with NETCOM & PM BES on
  - Emerging security guidelines
  - Reimbursable requirement for TNOSC support
  - Review of implementation plans
  - Site support
  - Developing a Master Migration Schedul
- Work Funding Issues

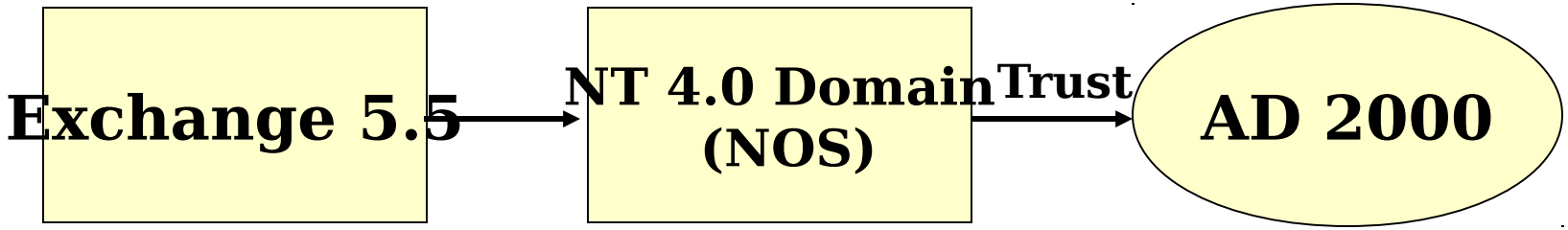




Robert.Bachert@us.army.mil

Back-UP Slides

New Exchange 5.5 Servers

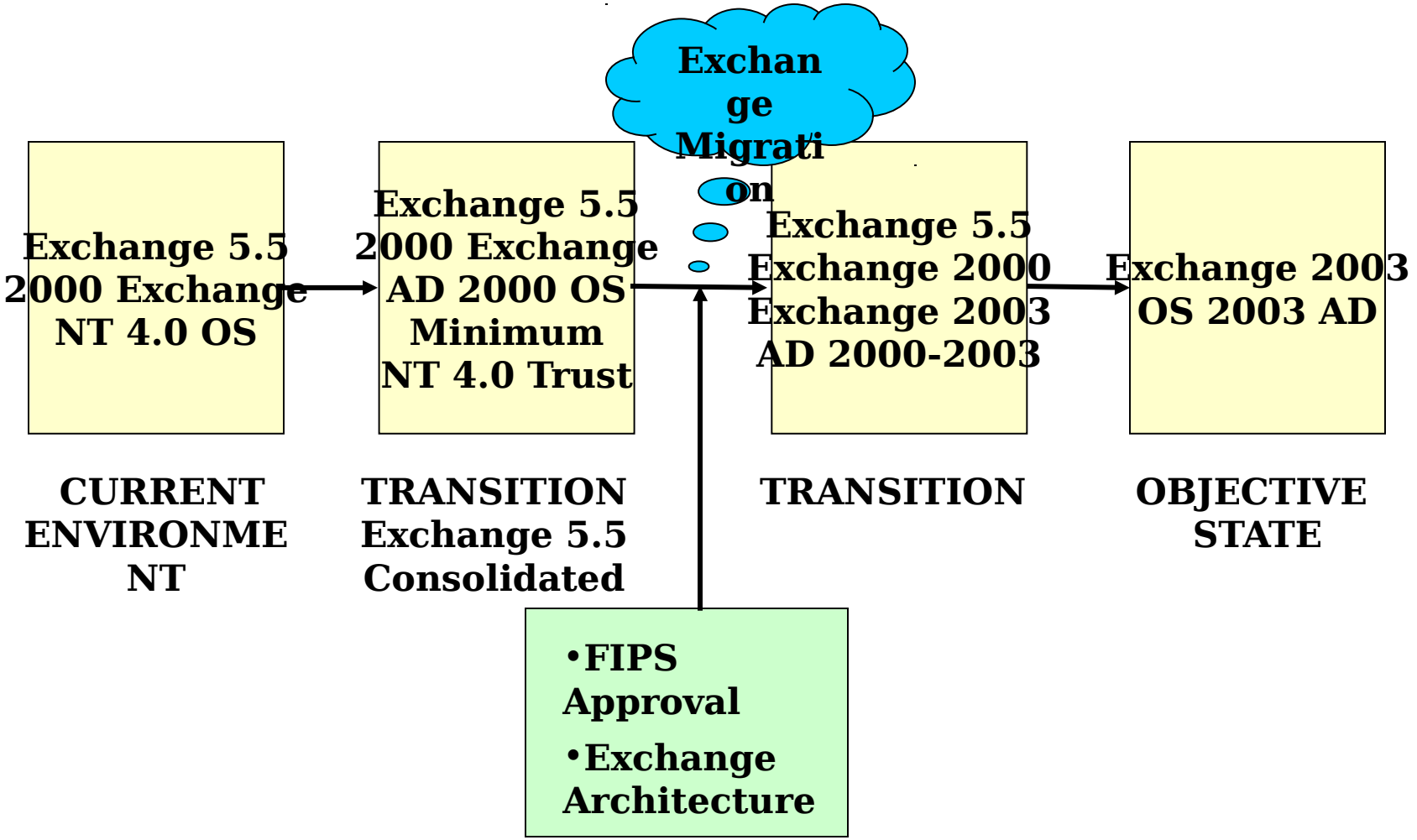


- 2000 OS
- NT 4.0 OS

- Accounts
- Users
- SID History

- Exchange 5.5 and NT 4.0 Domain Consolidation
- New exchange 5.5 servers build on 2000 OS
- All rebuilds of exchange 5.5 on 2000 OS
- Minimum NT 4.0 domain trust (one per installation)

Goal: Exchange 2003


Exchange Migration
Exchange 5.5 2000 Exchange NT 4.0 OS
Exchange 5.5 2000 Exchange AD 2000 OS Minimum NT 4.0 Trust
Exchange 5.5 Exchange 2000 Exchange 2003 AD 2000-2003
Exchange 2003 OS 2003 AD
CURRENT ENVIRONMENT
TRANSITION Exchange 5.5 Consolidated
TRANSITION
OBJECTIVE STATE
•FIPS Approval
•Exchange Architecture

Migration Order

- Pick installations that have consolidated NT 4.0 domains and Exchange 5.5 for first migration
- AD 2000 backbone and site Domains installed